

[Registered Entity Name]

NERC ID: [NCRXXXXX]

CIP-013-2 – Cyber Security – *Supply Chain Risk Management*

[QX] [20XX] Guided Self-Certification Worksheet

# Instructions

1. Populate the cover page by adding your Registered Entity name, NERC compliance registry (NCR) number, and the quarter and year indicated for the Guided Self-Certification in Align.
2. Complete the tasks listed under Assessment Guidance. Only complete tasks listed for the Requirements in scope.
3. Log into Align and complete your Guided Self-Certification response.
4. Where random sampling is required, use an objective tool such as Microsoft Excel or random.org. If you have questions, reference NERC’s [Compliance Monitoring and Enforcement Manual](https://www.nerc.com/pa/comp/CAOneStopShop/ERO%20Enterprise%20Compliance%20Monitoring%20and%20Enforcement%20Manual%20v6.pdf) (2021 Version 6, p. 151) or contact your Guided Self-Certification lead for assistance.
5. Submit the following to the Secure Evidence Locker (SEL):
	1. This completed worksheet; and
	2. The specific evidence annotated for the requested Requirements.
		1. Please use unique file names and identify which file(s) support each conclusion.
		2. Direct references and unique file names facilitate an expedited review of the Guided Self-Certification.
6. The Guided Self-Certification request in Align includes the monitoring period and the timeframe to perform the assessment and respond.
7. For the purpose of this document all capitalized terms have the meaning ascribed to them in the NERC *Glossary of Terms Used in NERC Reliability Standards* ([Available Here](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf)) unless otherwise indicated.

# Requirement

The scope of this CIP-013-2 Guided Self-Certification is listed below:

|  |  |
| --- | --- |
| CIP-013-2 Requirement | In Scope |
| **R1** | *Requirement is included within the scope of this SC* |
| **R2**  | *Requirement is not included within the scope of this SC* |
| **R3** | *Requirement is not included within the scope of this SC* |

# Assessment Guidance - Compliance

## R1

* + - 1. Provide the current version of the plan(s) to manage cyber security risk in the supply chain for high and medium impact BES Cyber Systems and their associated EACMS and PACS.

|  |
| --- |
| Evidence of Supply Chain Cyber Security Risk Management Plan(s) |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Provide the process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS. Please identify where the process(es) collectively result in the identification and assessment of cyber security risks to the BES from vendor products and services resulting from:

Procuring and installing vendor equipment and software; and

Transitions from one vendor or set of vendors to another vendor or set of vendors.

|  |
| --- |
| Evidence of Process(es) to Identify and Assess Cyber Security Risks |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Provide the process(es) used in the procurement of BES Cyber Systems and their associated EACMS and PACS. Please identify where the process(es) address the areas identified in Requirement R1 Part 1.2.1 through 1.2.6. If any of the areas identified in Part 1.2.1 through 1.2.6 were not applicable, provide evidence to demonstrate the reason(s) it is not applicable.

|  |
| --- |
| Evidence of Process(es) Used in the Procurement to Address R1.2 Topics  |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Do the supply chain risk management plan(s) evaluate value-added resellers and original equipment manufacturers with the identification and assessment of cyber security risks?

|  |
| --- |
| Entity Narrative  |
| Response: |

* + - 1. How are renewal agreements and/or service subscriptions considered within the documented supply chain risk management plan(s)?

|  |
| --- |
| Entity Narrative  |
| Response: |

* + - 1. How are the documented supply chain risk management plan(s) implemented for emergency related procurements?

|  |
| --- |
| Entity Narrative  |
| Response: |

## R2

Provide a list of all individuals, companies, or other external organizations the Responsible Entity, or its affiliates, procure products or services for high or medium impact BES Cyber Systems and their associated EACMS and PACS.

|  |
| --- |
| List of Persons, Companies, or Other External Organizations |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

For high and medium impact BES Cyber Systems and their associated EACMS and PACS, provide a list of each procurement of vendor products or services resulting from:

Procuring and installing vendor equipment and software; and

Transitions from one vendor(s) to another vendor(s) during the time period covered by this Self-Certification.

Please include:

Unique ID;

Vendor;

Associated BES Cyber System Impact Level;

Description of products or services by vendor or vendor transition;

Whether the procurement was for a vendor product; vendor service; or resulted in a vendor transition;

Identification & assessment start date;

Identification & assessment end date;

Procurement start date;

Procurement end date;

Cyber Asset Classification

\*\*Note\*\* - The list of procurements should include those completed and in progress. This request seeks information that would be submitted with the Evidence Request Tool “Procurement” tab request for information (version 7.0).

|  |
| --- |
| List of Procurements  |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Select a random sample from the procurements identified in (R2) step 2, above.
2. For each procurement selected in the sample above from (R2) step 3, provide evidence of the identification and assessment of cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from:
	* 1. Procuring and installing vendor equipment and software; and
		2. Transitions from one vendor(s) to another vendor(s).

|  |
| --- |
| Evidence of Identification and Assessment of Cyber Security Risks |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. For each procurement selected in the sample above from (R2) step 3, related to the products or services provided that pose cyber security risk, provide evidence of the implemented processes used in procuring for the areas identified in Requirement R1 Part 1.2.1 through 1.2.6. As applicable, please identify where the process(es) specifically addressed:
	1. Notification by the vendor of vendor-identified incidents;
	2. Coordination of responses to vendor-identified incidents;
	3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
	4. Disclosure by vendors of known vulnerabilities;
	5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and
	6. Coordination of controls for vendor-initiated remote access.

\*\*Note\*\* - If any of the areas are not applicable to the procurement, provide evidence to demonstrate the reason(s) it is not applicable.

|  |
| --- |
| Evidence of Addressing R1.2 Topics in Procurements |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Since October 1, 2020, have any applicable transitions from one vendor(s) to another vendor(s) occurred? If so, please briefly describe.

|  |
| --- |
| Entity Narrative  |
| Response:  |

## R3

* + - 1. Provide evidence demonstrating the supply chain cyber security risk management plan(s) specified in Requirement R1 were reviewed on or before the effective date of this Standard, and at least once every 15 calendar months thereafter.

|  |
| --- |
| Evidence of Review |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Provide evidence to demonstrate the CIP Senior Manager or delegate approved the supply chain cyber security risk management plan(s) specified in Requirement R1 on or before the effective of this Standard, and at least once every 15 calendar months thereafter. If a delegate approved the plan(s), provide evidence of the delegated authority pursuant to CIP-003-8 R4.

|  |
| --- |
| Evidence of Approval |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

# Assessment Guidance - Controls

**Controls Instructions:**

In this section of the document, WECC asks you to identify/describe the controls your entity put in place to mitigate the risk(s) addressed by this Standard. When WECC asks you to "provide associated evidence," you should provide any evidence (examples include checklists, processes, procedures, training, sign-in sheets, *etc*.) demonstrating your entity *created* a control and *implemented* the control.

If you have any questions, please reach out to internalcontrols@wecc.org.

**Controls Questions:**

1. Describe the controls your entity has to ensure an appropriate, accurate, and effective risk identification and assessment was performed for R1.1, and provide supporting evidence.
	1. Additionally, describe any controls your entity has in place to identify emerging security risks to the BES.

|  |
| --- |
| Narrative  |
| Response:(a)  |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Is a third-party service used to assist with identification and assessment of cyber security risks of vendors? If so:
	1. Identify the service(s) and briefly describe how the service supports the documented processes.
	2. Describe the controls your entity has implemented to ensure the third-party satisfactorily identified and assessed those risks and provide supporting evidence of performing the controls.

|  |
| --- |
| Narrative  |
| Response:(a)(b)  |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. If a vendor chooses not to adhere to one or more sub-parts of Part 1.2, describe how your entity would address the risk (e.g., controls or mitigations to ensure notification, coordination, disclosure of vendor-identified incidents, vulnerabilities, terminated access).

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Are vendor risk assessments monitored for change in risk over time and updated, regardless of procurement activities? If “yes,” please provide a narrative and supporting evidence for the control.

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Describe any controls your entity performs to determine if any transitions from one vendor to another vendor are scheduled to occur and provide supporting evidence.

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Does your entity use any automated controls to track periodic risk reviews? If “yes,” please describe the automated controls and supporting processes.

|  |
| --- |
| Narrative  |
| Response:  |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Does your entity have any controls to ensure supply chain risk management activities are integrated with other internal processes (e.g., change management, software patching, vulnerability assessments)? If “yes,” please describe the supporting processes.

|  |
| --- |
| Narrative  |
| Response:  |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. For procurements that do not meet the applicability of CIP-013 R1, are any of the supply chain risk management plan(s) protections afforded? If so, please briefly describe.

|  |
| --- |
| Narrative  |
| Response:  |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. What sources of information are monitored for current and emerging supply chain-related concerns and vulnerabilities for possible updates to the supply chain cyber security risk management plans developed in Requirement R1?

|  |
| --- |
| Narrative  |
| Response:  |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

# Evidence Submittal

Please submit the following evidence with the Guided Self-Certification response to the Secure Evidence Locker (SEL):

|  |  |
| --- | --- |
| CIP-013-2 Requirement | Evidence |
|  | This completed worksheet |
| **R1** | *Requirement is included within the scope of this SC:*Supply Chain Cyber Security Risk Management Plan(s)Process(es) to Identify and Assess Cyber Security RisksProcess(es) Used in the Procurement to Address R1.2 Topics |
| **R2**  | *Requirement is not included within the scope of this SC*List of Individuals, Companies, or Other OrganizationsList of ProcurementsIdentification and Assessment of Cyber Security RisksAddressing R1.2 Topics in Procurements |
| **R3** | *Requirement is not included within the scope of this SC*Review DocumentsApproval Documents |
| **As Applicable** | Controls Evidence (if provided in response to any *Assessment Guidance – Controls* questions) |

# Revision Table

|  |  |
| --- | --- |
| Revision Date | Description of Revision |
| 8/30/2021 | Initial version of CIP-013-1 Guided Self-Certification Worksheet |
| 11/28/2022 | Updated *Assessment Guidance – Compliance* questions to account for changes in CIP-013-2 (adding associated EACMS and PACS) |
| 2/28/2023 | Revisions include: * Reference to Compliance Monitoring and Enforcement Manual (version 6)
* Moved some questions from *Assessment Guidance – Compliance* to *Assessment Guidance – Controls* section
* Revised language in *Assessment Guidance – Controls* section
* Moved “Evidence Submittal” to end of worksheet
* Added Revision Table
 |